PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-350727
(43)Date of publication of application : 21.12.2001

(51)Int.Cl. G06F 15/00
G06F 13/00
G09C 1/00
G10K 15/02
H04L 9/10
H04L 9/32
H04N 7/16
H04N 7/173

(21)Application number : 2000-168549
(22)Date of filing : 06.06.2000

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : SAKIMURA TOSHIO
OKADA TAKESHI

(54) CONTENTS DISTRIBUTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To service the maintenance of contents possessed by a user after distribution in a contents distribution system utilizing a network.
SOLUTION: This system is provided with a server 100 for distributing contents are a client terminal 15 connected with this server on the network. The server 100 incorporates a contents key generating part 104 and a contents enciphering part 105 or the like and the client terminal 150 incorporates a second storage part 154 for receiving and storing contents distributed from the side of the server 100a user ID card 155 for transmitting a control signal to the side of the server 100 and a deciphering part 153 for deciphering the enciphered contents or the like.

CLAIMS

[Claim(s)]
[Claim 1]A contents distribution system which comprises a server which distributes contents characterized by comprising the following accompanied by an imagea soundetc.and a client terminal which receives contents which network connection was carried out to said serverand were distributed from this server. The 1st storage parts store in which said server accumulates said contents and contents identification information.

An extraction part which extracts said contents identification information from said 1st storage parts store.
A contents key generation part which generates a contents key for enciphering and deciphering said contents.
An encryption section which enciphers said contents using said contents key outputted from said contents key generation partAn accounting part which asks a user of a client terminal of a distribution destination for a remuneration which ****s to said contentsand performs accountingAn output of said encryption section is distributed to said client terminal through said networkHave a server message distribution processing part which outputs transmit information from said client terminal to said contents key generation part and said accounting partand said client terminalA client message distribution processing part which receives said distributed contentstransmits to the 2nd storage parts storetransmits a control signal from a user ID card to said serverand transmits a control signal from this server to this user ID cardThe 2nd storage parts store that accumulates said distributed contentsa decoding section which decodes said enciphered contents and is reproduceduser identification information which identifies apparatus which a user and a user useand said contents key.

[Claim 2]Said contents distribution systemwherein said client terminal is provided with still more nearly removable card reader/writer in a memory card which stored said contents in the contents distribution system according to claim 1.
[Claim 3]Claim 1 statement characterized by comprising the followingor the contents distribution system according to claim 2.
Said server is each user's User Information further.
Contents identification information of contents distributed to this user.
The Research and Data Processing Department which does database management of said contents key used for encryption of said contents.

[Claim 4]Said server in the contents distribution system according to claim 3 furtherContents attribute information which defined remuneration information and a utilization condition of contents as said 1st storage parts store is savedA contents distribution systemwherein said extraction part extracts said contents identification information and said contents attribute information from said 1st storage parts store and said Research and Data Processing Department manages this contents identification informationthis contents attribute informationsaid contents keyand said User Information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention consists of a contents server with which said

contents are accumulatedand a client terminal by which network connection was carried out to this serverconcerning the distribution system of contentssuch as music and a movieand relates to the contents distribution system which devised especially customer relations management and copyright protection.
[0002]
[Description of the Prior Art]Drawing 9 shows the functional block of the information distribution system known conventionally. In drawing 9the server by which 10 supplies contents to a userand 20 are user terminals. The Internet connectivity of the server 10 and the user terminal 20 is carried out. The contents accumulating part which the numerals 11-17 show the functional block of server 10 insideand stores contents with various numerals 11A fee collection manager and 17 are communication managers the apparatus key database which can refer to the apparatus key corresponding to apparatus ID in 14 corresponding to a contents encryption section in 13 corresponding to a contents key generation part in 12the apparatus encryption section which enciphers by an apparatus key 15and 16.
[0003]The numerals 21-24and 26 express the functional block of user terminal 20 inside. The remote processing manager whom the numerals 21 give general processing in connection with [with respect to a card reader/writer in the communication manager in the user terminal 20 and 22] distribution in 23the data accumulation part 24 remembers encryption data to beand 25 are IC cards. IC card 25 can be inserted now in a card reader / writer 22. 26 is a code decoding section which performs encryption and decryption of the information which accompanies contents and these contents.
[0004]Nowthere is a user's demand and the case where desired contents are downloaded to the user terminal 20 is considered. At this timethe server 10 takes out desired contents from the contents accumulating part 11and transmits contents to the contents encryption section 13. In the contents encryption section 13contents are enciphered using the contents key transmitted from the contents key generation part 12. Information original with contentsfor examplefee collectionthe expiration dateetc. are contained in the contents key.
[0005]The contents key generated by the contents and the contents key generation part 12 which were enciphered by the contents encryption section 13 is transmitted to the apparatus encryption section 15respectively. In the apparatus encryption section 15it is respectively enciphered further using an apparatus keyand contents and a contents key are sent to the user terminal 20 via the communication manager 17. An apparatus key is taken out from the apparatus key database 14. The apparatus key is beforehand written in the apparatus which a user possesses with apparatus ID at the time of factory shipmentsand can memorize the combination to the apparatus key database 14 further. Although a user can refer to apparatus IDany users are prevented from referring to an apparatus key. A user transmits apparatus ID to beforehand [of download] at a serverand the server 10 pulls out apparatus ID transmitted by the user and a corresponding apparatus key from the apparatus key database

14transmits to the apparatus encryption section 15and performs apparatus encryption.
[0006]In the user terminal 20the contents key and contents which were enciphered by the apparatus key are once sent to the data accumulation part 24 via the communication manager 21 of the user terminal 20. After the remote processing manager 23 checks that desired contents have been transmitted thoroughlythe accounting information currently recorded on IC card 25 is updatedand just fee collection is performed. Or after the server 10 checks that the user has received contents to be surethe fee collection manager 16 performs suitable accounting.
[0007]The contents accumulated in the data accumulation part 24 are transmitted to the code decoding section 26 at the time of reproduction. The apparatus key peculiar to the apparatus is embedded in the memory area which cannot be referred to from a user in the code decoding section 26and apparatus encryption of contents and a contents key is decoded first. Thenusing the contents key produced by decoding apparatus encryptioncontents encryption of contents is decoded and it is decoded by contents data suitable for a user's utilizing method.
[0008]As a contents distribution system relevant to this inventionwhat was indicatedfor example to JP11-328850A and JP2000-36781A is known.
[0009]
[Problem(s) to be Solved by the Invention]Howeveralthough the copyright of the contents which the user could obtain desired contents early and easilyand were distributed is protected by the conventional information distribution systemIt becomes only the only user terminal discriminable by apparatus ID that the contents which received can be usedand it cannot be used with a user terminal with different apparatus ID from this apparatus ID.
[0010]When contents have been disappeared by causessuch as failure of a user's memory storagein order to use these contents once againa user has to receive distributionafter paying a fee again.
[0011]Even if copying freely is accepted when the attribution information about contents changesand the term of validity of copyright goes outfor exampleIf there is no way a user can possess the contents data itself which exhibited the apparatus keyor canceled encryption of contents and was decodedthere is a problem that the decoded contents cannot be copied freely.
[0012]Thereforethe purpose of this invention makes it possible to receive distribution with the arbitrary client terminals by which network connection was carried out in a contents distribution system. The number of times is limitedand it enables it to receive re-distribution of contentswhen the contents in which the user received distribution have disappeared by a certain causewithout paying a fee. When attribution information from which the user received distributionsuch as copyright of contents and a remunerationis changedit becomes possible to improve user convenience because notify the attribution information of contents in response to a user's notice requests or a server notifies a user autonomously.
[0013]

[Means for Solving the Problem]In order to solve this technical problemthe invention of this invention according to claim 1In a contents distribution system which comprises a server which distributes contents accompanied by copyrightssuch as an image and a soundand a client terminal which receives contents which network connection was carried out to said serverand were distributed from this serverThe 1st storage parts store in which said server accumulates said contents and contents identification informationAn extraction part which extracts said contents identification information from said 1st storage parts storeA contents key generation part which generates a contents key for enciphering and deciphering said contentsA contents encryption section which enciphers said contents using said contents key outputted from said contents key generation partAn accounting part which asks a user of a client terminal of a distribution destination for a remuneration which ****s to said contentsand performs accountingAn output of said encryption section is distributed to said client terminal through said networkHave a server message distribution processing part which outputs transmit information from said client terminal to said contents key generation part and said accounting partand said client terminal receives said distributed contentsand transmits to the 2nd storage parts storeA client message distribution processing part which transmits a control signal from a user ID card to said serverand transmits a control signal from this server to this user ID cardThe 2nd storage parts store that accumulates said distributed contentsand a decoding section which decodes said enciphered contents and is reproducedIt is a contents distribution system which consists of a user ID card which stores User Information which consists of user identification information which identifies apparatus which a user and a user useand said contents keyand the card reader/writer part equipped with said user ID card.

[0014]contents of which a user expects distribution are enciphered by such composition using user ID and content ID -- **** -- if a user has a user ID cardany client terminals can receive contents distribution and copyright will also be protected.

[0015]The invention of this invention according to claim 2 equips a client terminal with a card reader/writer which can detach and attach a memory card further in claim 1. Reproducing contents stored in a memory card in other decoding reproduction devices by thiswhile contents etc. are storable in a memory card free is done so.

[0016]In claim 1 statement or the contents distribution system according to claim 2 the invention of this invention according to claim 3Said server provides the Research and Data Processing Department which does further database management of each user's User Informationcontents identification information of contents distributed to this userand said contents key used for encryption of said contents. By providing the Research and Data Processing Departmentthe invention of this invention according to claim 3 can manage user content IDthe newest distribution timea copyright terma remuneration (price) of copyrightthe number of times of distributiona contents keyetc. for every user. When contents

distributed to a user have disappeared by causessuch as hardware faultby thissince a server has managed a user's informationit becomes possible to re-distribute music in which this user received distribution.
[0017]In the contents distribution system according to claim 3 the invention of this invention according to claim 4Further said server to said 1st storage parts store Remuneration information on contentsSave contents attribute information which defined a utilization conditionsaid extraction part extracts said contents identification information and said contents attribute information from said 1st storage parts storeand said Research and Data Processing Department Said User InformationSaid contents identification informationsaid contents keyand said contents attribute information are managed.
[0018]When copyright of contents in which a user received distribution goes out by thisa server is notifying a user of copyright of contents having gone outand distributing a contents key to a user if neededA user can decode enciphered contents and can deal with it now freely.
[0019]
[Embodiment of the Invention]Hereafteran embodiment of the invention is described using drawing 1 - drawing 8.
[0020](Embodiment 1) Drawing 1 starts Embodiment 1 of the contents distribution system in this invention. In drawing 1300 is a server which distributes contents. The numerals 301302304105106and 107 express the internal function block of the server 300. The 1st storage parts store in which the numerals 301 accumulate contents and contents identification informationThe extraction part from which 302 extracts contents identification informationthe contents key generation part which generates the key which 304 uses for encryption of contentsThe contents encryption section which enciphers contents using the contents key to which 105 was outputted from the contents key generation partThe accounting part which 106 asks the user of the client terminal of a distribution destination for the remuneration which ****s to the distributed contentsand performs accounting107 is a server message distribution processing part which distributes the output of an encryption section to the client terminal 350 through said networkand outputs the transmit information from the client terminal 350 to a contents key generation part and the accounting part 106.
[0021]The numerals 351352153 and 154 express the internal function block of the client terminal 350. The numerals 351 receive the distributed contents and transmit to the 2nd storage parts storeThe client message distribution processing part which transmits the control signal from the user ID card 155 to the server 300and transmits the control signal from this server to the user ID card 155The card reader/writer which 352 equips with the user ID card 155The decoding section which decodes the code of contents in which 153 was distributedthe 2nd storage parts store that stores the contents to which 154 was distributedand 155 are user ID cards which store User Information which consists of user identification information which identifies the apparatus which a user and a user useand a contents key. This user ID card 155 is needed when a user receives

distribution.
[0022]About the contents distribution system constituted as mentioned abovethe operation is described hereafter. Nowa certain user demands distribution of desired contents of the server 300 using the client terminal 350distribution is receivedand the case where client terminal 350 smell contents are reproduced is considered. The contents key first used for contents encryption is created at the time of distribution. The copy generation information on a contents key is further added to contents key generation using the user ID currently recorded on the user ID card 155 which a user usesand content ID. The copy of a contents key is restricted by this. A contents key by general common key delivery which added ID informationfor example to the method of Diffie-Hellman. It is shared between the user ID card 155 and the contents key generation part 304 in secrecyand The user ID card 155A contents key can be intercepted from neither servers 300 other than contents key generation part 304 and other functional blocks of the client terminal 350 nor other network apparatus. Howeverthe contents key of various contents in which the user received distribution will be stored in the user ID card 155.
[0023]Nextthe scene which actually distributes is described. Firstthe extraction part 302 extracts content ID from the 1st storage parts store 301. The extracted content ID is sent to the contents key generation part 304. In generating a contents keyin the contents key generation part 304user ID is beforehand acquired from the user ID card 155. Nextthe contents key generation part 304 generates a contents key using content ID and user ID. A contents key is transmitted to the contents encryption section 105. From the 1st storage parts store 301it is transmitted to the contents encryption section 105and contents are enciphered in the contents encryption section 105. The enciphered contents are distributed to the client terminal 350 through the server message distribution processing part 107. The server message distribution processing part 107 will perform accounting which it notifies to the accounting part 106 and the accounting part 106 asks for the remuneration of contents to said userif the completion of distribution of said contents is checked.
[0024]In the client terminal 350the distributed contents are once saved at the 2nd storage parts store 154. Contents are enciphered by the contents key at this time. Mutual recognition is performed in order that apparatus with mutual user ID card 155 and decoding section 153 may confirm first whether it is a regular thingwhen reproducing contents. Only when it is able to be mutually checked by mutual recognition that it is regular apparatusa contents key is transmitted to the decoding section 153 from the user ID card 155. When a contents key is transmitted to the decoding section 153 from the user ID card 155For examplethe 1st common key is created between the user ID card 155 and the decoding section 153 using the key delivery of Diffie-Hellmanand using this 1st common keythe contents key itself is enciphered and it transmits. In the decoding section 153the contents key enciphered first after thatIt is decoded using the 1st common keythe contents by which contents encryption was carried out next are transmitted to the decoding section 153 from the 2nd storage parts store 154and

it is changed into the data which a code is decoded using a contents key and a user can use in the decoding section 153.
[0025]Use limitation information can also be added to a contents key. in this case -- when decoding contentsthe decoding part 153 refers to the use limitation information included in a contents key -- contents -- it is goodthough it decodes only when available.
[0026]As mentioned abovein the contents distribution system by this Embodiment 1it is enciphered using content ID and user IDand contents are transmitted to the client terminal 350 from the server 350. If a user has the user ID card 155 when he receives distributionevery client terminal can receive distribution of contents andmoreovercopyright will be protected.
[0027](Embodiment 2) Drawing 2 starts Embodiment 2 of the contents distribution system in this invention. In drawing 2400 is a server which distributes contentsand the composition of this server is almost the same as the server 300 shown in drawing 1.
[0028]450 is the client terminal by which network connection was carried out to the server. The numerals 351452 and 154 express the internal function block of the client terminal 450. The numerals 351 receive the distributed contents and transmit to the 2nd storage parts store 154The client message distribution processing part which transmits the control signal from the user ID card 155 to the server 300and transmits the control signal from the server 300 to this user ID card 155and 452 The user ID card 155The card reader/writer equipped with the memory card 156the 2nd storage parts store that stores the contents to which 154 was distributedand 155 are user ID cards which store User Information which consists of user identification information which identifies the apparatus which a user and a user useand a contents key. This user ID card 155 is needed when a user receives distribution. 156 is a memory card which can store the contents which received distributionand the contents key which is needed for decoding of contents. 157 is a decoding reproduction device and can equip with the memory card 156.
[0029]About the contents distribution system constituted as mentioned abovethe operation is described hereafter. The scene which copies the contents key for decoding the contents to which a certain user was distributed nowand these contents to the memory card 156 is considered. In this casecontents shall be saved at the 2nd storage parts store 154and the contents key shall already be stored in the user ID card 155. The copy generation information on a contents key itself [this] shall be added to the contents key. Firstcontents are copied to the memory card 156 in the state where it was enciphered. The copy to the memory card 156 of the contents enciphered may be performed freely. Nexta contents key is copied to the memory card 156.
[0030]Drawing 5 shows the flow chart of the processing 600 which copies a contents key to the memory card 156. The processing 600 comprises the processings 601-606. In the processing 601mutual recognition which checks that mutual apparatus is regular apparatus between the user ID card 155 and the

memory card 156 is performed first. When said mutual recognition goes wrongthe copy to the memory card 156 is stopped and the processing 600 is ended. If it succeeds in said mutual recognitionin the processing 602the user ID card 155 and the memory card 156 will perform key delivery of Diffie-Hellmanand the 2nd common key for transmitting a contents key safely between the user ID card 155 and the memory card 156 will be created. Nextin the processing 603it checks that the copy generation of this contents key is below N with reference to the contents key stored in the user ID card 155. HereN is zero or more integers and one optimal value in each contents distribution system is chosen. Processing is ended when said copy generation value is above (N+1). When said copy generation is below Nit progresses to the next processing. In the processing 6041 is added to the copy generation value of a contents key. Nextit enciphers using said 2nd common key that created the contents key of the user ID card 155 by the processing 602 in the processing 605. Nextin the processing 606a contents key is transmitted to the memory card 156 from the user ID card 155and a contents key is decoded using said 2nd common key stored in the memory card 156. This decoded contents key is stored in the field which a user cannot read. By recording a contents key on the field which cannot be reada user prevents an illegal copy.

[0031]Contents and a contents key are recorded on the memory card 156 by the above procedure. By equipping the decoding reproduction terminal 157 with the memory card 156when there is no user ID card 155contents can be changed into a user's available data by the function decoding of the decoding reproduction terminal 157.

[0032]Use limitation information can also be added to a contents key. in this case -- when decoding contentsthe decoding reproduction terminal 157 refers to the use limitation information included in a contents key -- contents -- it is goodthough it decodes only when available.

[0033]As mentioned abovethe contents distribution system by this Embodiment 3 stores a contents key required for the decipherment of the contents and the code which were enciphered by the memory card 156. The copy generation information on the contents key itself is added to the contents keyand the copy frequency of a contents key is restricted. A contents key is storing in the field which a user cannot readand prevents copying a contents key unjustly. Therebythe user can restore contents to the data which a user can use by equipping the decoding reproduction terminal 157 with the memory card 156.

[0034](Embodiment 3) Drawing 3 starts Embodiment 3 in the contents distribution system of this invention. The server to which 500 distributes contents in drawing 3the 1st storage parts store in which 301 stores contents and contents identification informationThe extraction part from which 102 extracts contents identification informationand 103 for every user User ID and the distributed contentsAnd the Research and Data Processing Department holding informationincluding a contents key etc.the contents key generation part which generates the contents key which uses 104 for encryption of contentsThe contents encryption section as which 105 enciphers contentsthe accounting part

which 106 asks the user of a distribution destination for the remuneration which ****s to the distributed contentsand performs accounting107 is a server message distribution processing part which distributes the output of an encryption section to the client terminal 550 through a networkand outputs the transmit information from a client terminal to a contents key generation part and the accounting part 106.

[0035]The numerals 551152153 and 154 express the internal function block of the client terminal 550. 551 receives the distributed contentstransmits to the 2nd storage parts storeand transmits the control signal from the user ID card 155 to the server 500 sideThe client message distribution processing part which transmits the control signal from the server 500 side to the user ID card 155and 152 The user ID card 155The card reader/writer equipped with the memory card 156the decoding section which decodes the code of contents in which 153 was distributedThe 2nd storage parts store that stores the contents to which 154 was distributedand 155 are the user ID cards 155 which store User Information which consists of user identification information which identifies the apparatus which a user and a user useand a contents key. The user ID card 155 is needed when a user receives distribution. 156 is a memory card which can store the contents which received distributionand the contents key which is needed for decoding of contents. 157 is a decoding reproduction device and can equip with the memory card 156.

[0036]Drawing 8 is an example of the user information data base managed in the Research and Data Processing Department 103. The Research and Data Processing Department 103 manages user IDcontent ID and the newest distribution timea copyright termthe contents expiration datea pricethe number of times of distributioncontents key informationetc. like Embodiment 1 for every user who provides distribution service.

[0037]About the contents distribution system constituted as mentioned abovethe operation is described hereafter. About the scene which actually distributesit is almost the same as Embodiment 1. In the server 500as shown in drawing 8database management of User Informationsuch as All Users's contents distributing hysteresis informationis carried out. The server 500 enables it to re-distribute the contents in which the user already received distribution. Herewhen only the enciphered content saved at the 2nd storage parts store 154 etc. has brokencontents encryption may be carried outusing once again the contents key used for the last distribution. Howeverwhen the contents key has brokeneven if it enciphers by the same contents keysince the user cannot decodehe creates the 2nd different contents key from what disappeared between the user ID card 155 and the contents key generation part 104. Thencontents are enciphered by the 2nd contents key and it distributes to a user. By managing the creation history of a contents key in the Research and Data Processing Department 103a user restricts the number of times of contents key creation to the contents which received distributionand prevents an illegal copy.

[0038]The processing 700 of drawing 6 expresses the flow of processing in the

case of performing re-distribution with the user sidewhen contents have disappearedfor example by hardware fault. The processing 700 is constituted from the processing 701 by the processing 708. Firsta user accesses the server 500. Nextin the processing 701mutual recognition which checks that each is regular apparatus between the contents key generation part 104 and the user ID card 155 is performed. The processing 700 is ended when attestation goes wrong. If it succeeds in attestationa user will perform next the report shown in the processing 702. A user tells having damaged the cardand if you would like to re-distribute a certain contents which have disappeared nowhe will tell the server 500 here. The distribution music hysteresis information in the user information data base shown in drawing 8 in the processing 703 is referred to. In the processing 704the old number of times of distribution to the contents as which the user is demanding distribution is checkedif the old number of times of distribution is M or less timesa distribution request will be permittedif it is more than a time (M+1)a distribution request will be rejected and the processing 700 will be ended. M considers it as one or more integers hereand one value which becomes the best for each contents distribution system is chosen. Nextin the processing 705the 2nd contents key is distributed by the key delivery of Diffie-Hellman between the contents key generation part 104 and the user ID card 155. In the processing 706contents are enciphered using the 2nd contents key and it progresses to the next processing. In the processing 707the enciphered contents are re-distributed and 1 is added to the number of times of distribution of contents of a user's contents distributing hysteresis information in the processing 708.

[0039]As mentioned abovethe contents distribution system by this Embodiment 3 manages the information which distributed the server to the user or this user. Since the server has managed a user's information when the contents distributed to the user have disappeared by causessuch as hardware faultit makes it possible to re-distribute the music in which this user received distribution.

[0040](Embodiment 4) Drawing 4 starts Embodiment 4 of the contents distribution system in this invention. In drawing 4100 is a server which distributes contents and the numerals 101102103104105106and 107 express the internal function block of the server 100. The 1st storage parts store in which 101 stores contents and contents identification information (followingcontent ID)and content ID [as opposed to / according to a user's distribution request / the contents of a user desire in 102]The extraction part which extracts the contents attribute information showing a copyright terma remunerationetc. of contentsand 103 for every user A user's identification information (followinguser ID)The Research and Data Processing Department holding the distributed contents and informationincluding the contents key of these contentsetc.The contents key generation part which generates the contents key which uses 104 for encryption of contentsThe accounting part which performs demand processing for the contents encryption section as which 105 enciphers contentsand the remuneration which ****s to the contents to which 106 was distributed to the user of a distribution destinationand 107 are message distribution processing parts

which perform message distribution processing in a server.
[0041]The numerals 150 are the client terminals by which network connection was carried out to the server. The numerals 151152153and 154 express the internal function block of the remote terminal 150. The client message distribution processing part in which 151 performs message distribution processing by the side of a client terminalThe card reader/writer by which 152 equips a client terminal with a user ID card or the memory card 156The decoding section in which 153 decodes the enciphered contentsthe 2nd storage parts store in which 154 stores the enciphered contentsA memory card and 157 are decoding reproduction devicesandas for the user ID card for which 155 is needed when a user receives distributionand 156can equip with the memory card 156.
[0042]Drawing 8 is an example of the user information data base managed in the Research and Data Processing Department 103. The Research and Data Processing Department 103 manages user IDcontent ID and the newest distribution timea copyright termthe contents expiration datea pricethe number of times of distributioncontents key informationetc. for every user who provides distribution service. About the contents distribution system constituted as mentioned abovethe operation is described below.
[0043]Drawing 7 expresses the flow of the processing 800 when the copyright of contents goes out. The processing 800 comprises the processings 801-807. Firstin the processing 801the information on copyright is transmitted to the Research and Data Processing Department 103and it is reflected in a user information data base in the Research and Data Processing Department 103. Nextin the processing 802it is judged whether the controlling method of the distributed contents is automaticor it waits for a user's directions. When a controlling method is automatic (Yes)it shifts to the processing 804. After in (No) case the server 100 recognizes that the user accessed the server 100 for the first time since the attribution information of contents changes in the processing 803it shifts to the processing 804. [whose controlling method was not automatic] In the processing 804it tells a user that the copyright term of contents expired. In the processing 805as for a usercarrying out encryption release tells the server 100 whether lends and there is. Processing is ended to (No) case without the necessity for code release.
[0044]When a user demands encryption release (Yes)it shifts to the processing 806. In the processing 806the server 100 is stored in the Research and Data Processing Department 103and transmits the contents key of said contents to a user. At this timethe contents key which received distribution transmitswithout enciphering so that a user can treat freely. The user can decode contents freely using the contents key. Therebywhen copyright goes outa user decodes the code of contentsand after he changes into the data which a user can useit becomes possible to copy freely. Also in the case of the copyright piece shown by this embodimenta remuneration may not be made not to perform processing 800when it must pay. In this casewhen a remuneration changes to 0 yensuppose that processing 800 can be performed.

[0045]The contents distribution system by Embodiment 4 manages attribution information which the server distributed to the usersuch as a remuneration of contentsand copyright. When the copyright of the contents distributed to the user goes outa user is notified of a server and it transmits a contents key. If a contents key is usedthe encryption release of contents of a user will be attained. From these thingsthe server can maintain use restriction release of the contents distributed to the user.

[0046]

[Effect of the Invention]The contents of whichas for this inventiona user expects distribution are enciphered using user ID and content ID so that clearly from the place explained above. If a user has the user ID card 155any client terminals can receive contents distribution and copyright will also be protected.

[0047]moreover -- when this invention manages User Information by a server and the user has disappeared contents in a certain forma server limits the number of times -- contents -- re--- it can distribute.

[0048]Whenas for this inventionthe copyright of the contents in which the user received distribution goes outa server is notifying a user of the copyright of these contents having gone outand distributing a contents key to a user if neededA user can decode the enciphered contents and can deal with it now freely. Providing the contents distribution system whose convenience of the user who receives distribution improved by these is done so.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]The functional block diagram of the contents distribution system concerning the embodiment of the invention 1

[Drawing 2]The functional block diagram of the contents distribution system concerning the embodiment of the invention 2

[Drawing 3]The functional block diagram of the contents distribution system concerning the embodiment of the invention 3

[Drawing 4]The functional block diagram of the contents distribution system concerning the embodiment of the invention 4

[Drawing 5]The flow chart used for the explanation in the case of copying a contents key to the memory card in the contents distribution system of this invention

[Drawing 6]The flow chart explaining the re-distribution by card breakage in the contents distribution system of this invention

[Drawing 7]The flow chart used for the explanation in the case of the copyright expiration in the contents distribution system of this invention

[Drawing 8]The figure showing the table of an example of the User Information management data base in the contents distribution system of this invention

[Drawing 9]The functional block diagram explaining an example of the conventional

contents distribution system
[Description of Notations]
10100300400500 Server
11 Contents accumulating part
14 Apparatus key database
15 Apparatus encryption section
16 Fee collection manager
17 and 21 Communication manager
20150350450550 client terminals
23 Remote processing manager
24 Data accumulation part
25 IC card
101301 The 1st storage parts store
102302 Extraction part
103 Research and Data Processing Department
104 and 12304 Contents key generation part
105 and 13 Contents encryption section
106 Accounting part
107 Server message distribution processing part
151351551 Client message distribution processing part
22152352452 A card reader/writer
153 Decoding section
154 The 2nd storage parts store
155 User ID card
156 Memory card
157 Decoding reproduction terminal

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－350727
（P2001－350727A）
(43)公開日　平成13年12月21日(2001.12.21)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ 15/00	３３０Ｚ	５Ｂ０８５
				３３０Ｅ	５Ｃ０６４
	13/00	５４０	13/00	５４０Ｓ	５Ｊ１０４
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ 1/00	６６０Ａ	
				６６０Ｅ	

審査請求　未請求　請求項の数４　ＯＬ　（全 11 頁）　最終頁に続く

(21)出願番号　特願2000－168549(P2000－168549)

(22)出願日　平成12年６月６日(2000.6.6)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　崎村　俊夫
大阪府門真市大字門真1006番地　松下電器産業株式会社内

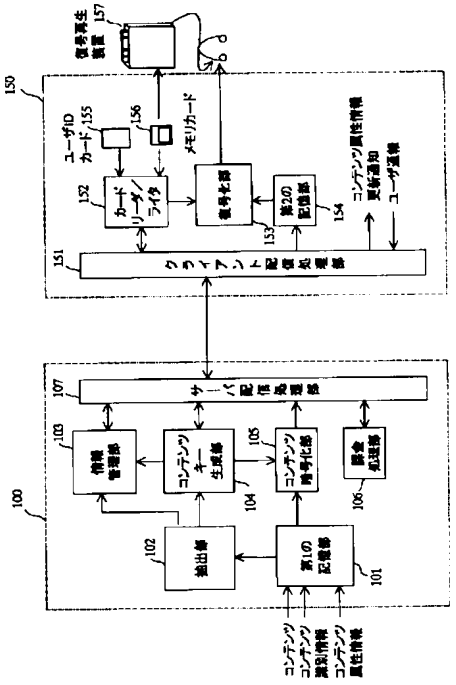
(72)発明者　岡田　健
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

最終頁に続く

(54)【発明の名称】　コンテンツ配信システム

(57)【要約】
【課題】　ネットワークを利用したコンテンツ配信システムで、配信後にユーザーがもつコンテンツのメンテナンスサービスが実施可能なシステムを実現する。
【解決手段】　コンテンツを配信するサーバ１００およびこれとネットワーク接続されたクライアント端末１５０とを備える。サーバ１００にはコンテンツキー生成部１０４、コンテンツ暗号化部１０５などが内蔵され、クライアント端末１５０にはサーバ１００側から配信されたコンテンツを受信して記憶する第２の記憶部１５４、サーバ１００側に制御信号を送信するユーザＩＤカード１５５、暗号化されたコンテンツを復号する復号化部１５３などが内蔵されている。



【特許請求の範囲】

【請求項１】　映像や音声などを伴ったコンテンツを配信するサーバと、前記サーバとネットワーク接続され、該サーバから配信されたコンテンツを受信するクライアント端末とで構成されるコンテンツ配信システムにおいて、前記サーバは、前記コンテンツおよびコンテンツ識別情報を蓄積する第１の記憶部と、前記第１の記憶部から前記コンテンツ識別情報を抽出する抽出部と、前記コンテンツを暗号化および暗号解読するためのコンテンツキーを生成するコンテンツキー生成部と、前記コンテンツキー生成部より出力された前記コンテンツキーを用いて前記コンテンツを暗号化する暗号化部と、前記コンテンツに相応する対価を配信先のクライアント端末のユーザに対して請求し課金処理を行う課金処理部と、前記暗号化部の出力を、前記ネットワークを通じて前記クライアント端末に配信し、前記クライアント端末からの送信情報を前記コンテンツキー生成部と前記課金処理部に出力するサーバ配信処理部とを備え、前記クライアント端末は、前記配信されたコンテンツを受信して第２の記憶部に送信し、ユーザＩＤカードからの制御信号を前記サーバに送信し、該サーバからの制御信号を該ユーザＩＤカードに送信するクライアント配信処理部と、前記配信されたコンテンツを蓄積する第２の記憶部と、前記暗号化されたコンテンツを復号し再生する復号化部と、ユーザやユーザの使用する機器を識別するユーザ識別情報と前記コンテンツキーとからなるユーザ情報を格納するユーザＩＤカードと、前記ユーザＩＤカードを装着するカードリーダ／ライタ部とからなることを特徴とするコンテンツ配信システム。

【請求項２】　請求項１記載のコンテンツ配信システムにおいて、前記クライアント端末はさらに、前記コンテンツを格納したメモリカードが着脱可能なカードリーダ／ライタを備えることを特徴とする前記コンテンツ配信システム。

【請求項３】　請求項１記載もしくは請求項２記載のコンテンツ配信システムにおいて、前記サーバは、さらに各ユーザのユーザ情報と、該ユーザに配信したコンテンツのコンテンツ識別情報と、前記コンテンツの暗号化に用いた前記コンテンツキーとをデータベース管理する情報管理部を設けることを特徴とする前記コンテンツ配信システム。

【請求項４】　請求項３に記載のコンテンツ配信システムにおいて、前記サーバはさらに、前記第１の記憶部にコンテンツの対価情報や利用条件を定義したコンテンツ属性情報を保存し、前記抽出部は前記第１の記憶部から前記コンテンツ識別情報と前記コンテンツ属性情報とを抽出し、前記情報管理部は該コンテンツ識別情報と、該コンテンツ属性情報と、前記コンテンツキーと、前記ユーザ情報とを管理することを特徴とするコンテンツ配信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、音楽や映画などのコンテンツの配信システムに関し、例えば前記コンテンツが蓄積されているコンテンツサーバと、このサーバとネットワーク接続されたクライアント端末とからなり、特に顧客管理と著作権保護を講じたコンテンツ配信システムに関する。

【０００２】

【従来の技術】図９は従来知られている情報配信システムの機能ブロックを示す。図９において、１０はユーザにコンテンツを供給するサーバ、２０はユーザ端末である。サーバ１０とユーザ端末２０は、インターネット接続されている。符号１１から１７がサーバ１０内部の機能ブロックを示し、符号１１はさまざまなコンテンツを格納するコンテンツ蓄積部、１２はコンテンツキー生成部、１３はコンテンツ暗号化部、１４は機器ＩＤに対応する機器キーを参照できる機器キーデータベース、１５は機器キーで暗号化を行う機器暗号化部、１６は課金マネージャ、１７は通信マネージャである。

【０００３】符号２１～２４および２６が、ユーザ端末２０内部の機能ブロックを表す。符号２１は、ユーザ端末２０における通信マネージャ、２２はカードリーダ／ライタ、２３は配信に関わる全般的な処理を行うリモート処理マネージャ、２４は暗号化データを記憶しておくデータ蓄積部、２５はＩＣカードである。ＩＣカード２５はカードリーダ／ライタ２２に挿入できるようになっている。２６はコンテンツ及び該コンテンツに付随する情報の暗号化・復号化を行う暗号復号化部である。

【０００４】いま、ユーザの要求があり、所望のコンテンツをユーザ端末２０にダウンロードする場合を考える。このときサーバ１０はコンテンツ蓄積部１１から所望のコンテンツを取り出し、コンテンツをコンテンツ暗号化部１３に送信する。コンテンツ暗号化部１３では、コンテンツキー生成部１２から送信されたコンテンツキーを用いて、コンテンツの暗号化を行う。コンテンツキーには、コンテンツ独自の情報、たとえば、課金，使用期限などが含まれている。

【０００５】コンテンツ暗号化部１３で暗号化されたコンテンツおよびコンテンツキー生成部１２で生成されたコンテンツキーは、それぞれ機器暗号化部１５に送信される。機器暗号化部１５において、コンテンツおよびコンテンツキーは、各々更に機器キーを用いて暗号化され、通信マネージャ１７を経由して、ユーザ端末２０に送られる。機器キーは、機器キーデータベース１４から取り出される。機器キーは、機器ＩＤとともに、ユーザが所持する機器に、あらかじめ工場出荷時に書き込んでおき、さらに機器キーデータベース１４にその組み合わせを記憶しておくことができる。機器ＩＤはユーザが参照することができるが、機器キーは、いかなるユーザも

参照できないようにしておく。ユーザは、ダウンロードの事前に機器ＩＤをサーバに送信し、サーバ１０は、ユーザから送信された機器ＩＤと対応する機器キーを機器キーデータベース１４から引き出し、機器暗号化部１５に送信し、機器暗号化を行う。

【０００６】ユーザ端末２０では、機器キーで暗号化されたコンテンツキーおよびコンテンツは、ユーザ端末２０の通信マネージャ２１を経由して一旦データ蓄積部２４に送られる。リモート処理マネージャ２３は、完全に所望のコンテンツが送信されたことを確認した後、ＩＣカード２５に記録されている課金情報を更新し、正当な課金が行われる。もしくは、サーバ１０がユーザが確かにコンテンツが受信できたことを確認した後、課金マネージャ１６が適切な課金処理を行う。

【０００７】再生時、データ蓄積部２４に蓄積されたコンテンツは、暗号復号化部２６に送信される。暗号復号化部２６ではユーザから参照することができないメモリ領域にその機器固有の機器キーが埋め込んであり、まずコンテンツ及びコンテンツキーの機器暗号化を復号する。その後、機器暗号化を復号して得られたコンテンツキーを用いて、コンテンツのコンテンツ暗号化を復号し、ユーザの利用方法に適したコンテンツデータに復号される。

【０００８】なお本発明に関連するコンテンツ配信システムとしては、例えば特開平１１－３２８８５０号公報、特開２０００－３６７８１号公報に記載されたものが知られている。

【０００９】

【発明が解決しようとする課題】しかしながら、従来の情報配信システムでは、ユーザは所望のコンテンツを早くしかも簡単に入手でき、また、配信されたコンテンツの著作権は保護されるが、受信したコンテンツを利用できるのは、機器ＩＤで識別できる唯一のユーザ端末のみとなり、該機器ＩＤと異なる機器ＩＤを持つユーザ端末では利用できない。

【００１０】また、ユーザの記憶装置の故障などの原因でコンテンツを消失してしまったとき、もう一度該コンテンツを利用するには、ユーザは再び料金を支払った上で、配信を受けなければならない。

【００１１】さらに、コンテンツに関する属性情報が変化した場合、例えば著作権の有効期限が切れた場合に、コピーを自由に行うことが認められたとしても、機器キーを公開するか、コンテンツの暗号化を解除し、復号されたコンテンツデータそのものをユーザが所持できる方法がなければ、復号されたコンテンツを自由にコピーできないという問題がある。

【００１２】したがって、この発明の目的は、コンテンツ配信システムにおいて、ネットワーク接続された任意のクライアント端末で配信を受けることを可能とする。また、ユーザが配信を受けたコンテンツが何らかの原因で消失してしまった場合、回数を限定して、料金を支払うことなくコンテンツの再配信を受けることができるようにする。また、ユーザが配信を受けたコンテンツの著作権や対価などの属性情報が変更された場合、ユーザの通知要求を受けてコンテンツの属性情報を通知したり、サーバが自律的にユーザへ通知したりすることで、ユーザ利便性を向上することが可能となる。

【００１３】

【課題を解決するための手段】この課題を解決するために、本発明の請求項１記載の発明は、映像や音声などの著作権を伴ったコンテンツを配信するサーバと、前記サーバとネットワーク接続され、該サーバから配信されたコンテンツを受信するクライアント端末とで構成されるコンテンツ配信システムにおいて、前記サーバは、前記コンテンツおよびコンテンツ識別情報を蓄積する第１の記憶部と、前記第１の記憶部から前記コンテンツ識別情報を抽出する抽出部と、前記コンテンツを暗号化および暗号解読するためのコンテンツキーを生成するコンテンツキー生成部と、前記コンテンツキー生成部より出力された前記コンテンツキーを用いて前記コンテンツを暗号化するコンテンツ暗号化部と、前記コンテンツに相応する対価を配信先のクライアント端末のユーザに対して請求し課金処理を行う課金処理部と、前記暗号化部の出力を、前記ネットワークを通じて前記クライアント端末に配信し、また前記クライアント端末からの送信情報を前記コンテンツキー生成部と前記課金処理部に出力するサーバ配信処理部とを備え、前記クライアント端末は、前記配信されたコンテンツを受信して第２の記憶部に送信し、ユーザＩＤカードからの制御信号を前記サーバに送信し、該サーバからの制御信号を該ユーザＩＤカードに送信するクライアント配信処理部と、前記配信されたコンテンツを蓄積する第２の記憶部と、前記暗号化されたコンテンツを復号し再生する復号化部と、ユーザやユーザの使用する機器を識別するユーザ識別情報と前記コンテンツキーとからなるユーザ情報を格納するユーザＩＤカードと、前記ユーザＩＤカードを装着するカードリーダ／ライタ部とからなるコンテンツ配信システムである。

【００１４】こうした構成によって、ユーザが配信を希望するコンテンツは、ユーザＩＤとコンテンツＩＤとを用いて暗号化されているも、ユーザはユーザＩＤカードがあれば、いかなるクライアント端末でもコンテンツ配信を受けることができ、著作権も保護される。

【００１５】本発明の請求項２記載の発明は請求項１において、クライアント端末にはさらにメモリカードの着脱が自在なカードリーダ／ライタを備える。これによって、メモリカードにコンテンツ等を自在に格納できるとともに、メモリカードに格納したコンテンツを他の復号再生装置において再生することが奏される。

【００１６】本発明の請求項３記載の発明は、請求項１

記載もしくは請求項２記載のコンテンツ配信システムにおいて、前記サーバはさらに、各ユーザのユーザ情報と、該ユーザに配信したコンテンツのコンテンツ識別情報と、前記コンテンツの暗号化に用いた前記コンテンツキーとをデータベース管理する情報管理部を設けるものである。本発明の請求項３記載の発明は情報管理部を設けることにより、ユーザ毎に、ユーザコンテンツＩＤ、最新の配信日時、著作権期限、著作権の対価（価格）、配信回数、コンテンツキーなどを管理することができる。これにより、ユーザに配信したコンテンツが、ハードウェア故障などの原因によって消失してしまった場合、サーバはユーザの情報を管理しているので、該ユーザが配信を受けた曲を再配信することが可能となる。

【００１７】本発明の請求項４記載の発明は、請求項３に記載のコンテンツ配信システムにおいて、前記サーバはさらに、前記第１の記憶部にコンテンツの対価情報や、利用条件を定義したコンテンツ属性情報を保存し、前記抽出部は前記第１記憶部から前記コンテンツ識別情報と前記コンテンツ属性情報とを抽出し、前記情報管理部は前記ユーザ情報と、前記コンテンツ識別情報と、前記コンテンツキーと、前記コンテンツ属性情報とを管理するものである。

【００１８】これによって、ユーザが配信を受けたコンテンツの著作権が切れた場合、サーバはユーザにコンテンツの著作権が切れたことを告知し、必要に応じてコンテンツキーをユーザに配布することで、ユーザは暗号化されたコンテンツを復号し、自由に取り扱うことができるようになる。

【００１９】

【発明の実施の形態】以下、本発明の実施の形態について、図１～図８を用いて説明する。

【００２０】（実施の形態１）図１は本発明におけるコンテンツ配信システムの実施の形態１に係る。図１において３００はコンテンツを配信するサーバである。符号３０１，３０２，３０４，１０５，１０６および１０７がサーバ３００の内部機能ブロックを表す。符号３０１はコンテンツとコンテンツ識別情報とを蓄積する第１の記憶部、３０２はコンテンツ識別情報を抽出する抽出部、３０４はコンテンツの暗号化に用いる鍵を生成するコンテンツキー生成部、１０５はコンテンツキー生成部より出力されたコンテンツキーを用いてコンテンツを暗号化するコンテンツ暗号化部、１０６は配信されたコンテンツに相応する対価を配信先のクライアント端末のユーザに対し請求し課金処理を行う課金処理部、１０７は暗号化部の出力を、前記ネットワークを通じてクライアント端末３５０に配信し、またクライアント端末３５０からの送信情報をコンテンツキー生成部と課金処理部１０６に出力するサーバ配信処理部である。

【００２１】符号３５１，３５２，１５３および１５４が、クライアント端末３５０の内部機能ブロックを表す。符号３５１は配信されたコンテンツを受信して第２の記憶部に送信し、ユーザＩＤカード１５５からの制御信号をサーバ３００に送信し、該サーバからの制御信号をユーザＩＤカード１５５に送信するクライアント配信処理部、３５２はユーザＩＤカード１５５を装着するカードリーダ／ライタ、１５３は配信されたコンテンツの暗号を復号する復号化部、１５４は配信されたコンテンツを格納する第２の記憶部、１５５はユーザやユーザの使用する機器を識別するユーザ識別情報とコンテンツキーとからなるユーザ情報を格納するユーザＩＤカードである。このユーザＩＤカード１５５は、ユーザが配信を受ける際に必要となる。

【００２２】以上のように構成されたコンテンツ配信システムについて、以下、その動作を述べる。いま、あるユーザがクライアント端末３５０を用いてサーバ３００に所望のコンテンツの配信を要求し、配信を受け、クライアント端末３５０においコンテンツを再生する場合を考える。配信時、初めにコンテンツ暗号化に用いるコンテンツキーを作成する。コンテンツキー生成には、ユーザが使用するユーザＩＤカード１５５に記録されているユーザＩＤと、コンテンツＩＤとを用い、さらに、コンテンツキーのコピー世代情報を付加する。このことで、コンテンツキーのコピーを制限する。コンテンツキーは、例えばＤｉｆｆｉｅ－ＨｅｌｌｍａｎのＩＤ情報を付加した一般的な共有鍵配送によって、ユーザＩＤカード１５５とコンテンツキー生成部３０４とで秘密裡に共有され、ユーザＩＤカード１５５と、コンテンツキー生成部３０４以外のサーバ３００およびクライアント端末３５０の他の機能ブロックや、ネットワークの他の機器からは、コンテンツキーを盗聴することはできない。しかるにユーザＩＤカード１５５には、ユーザが配信を受けた様々なコンテンツのコンテンツキーが格納されることになる。

【００２３】次に、実際に配信を行う場面について述べる。まず、抽出部３０２が、コンテンツＩＤを第１の記憶部３０１から抽出する。抽出されたコンテンツＩＤは、コンテンツキー生成部３０４に送られる。コンテンツキー生成部３０４では、コンテンツキーを生成するにあたり、あらかじめユーザＩＤを、ユーザＩＤカード１５５より取得しておく。次にコンテンツキー生成部３０４は、コンテンツＩＤと、ユーザＩＤとを用いて、コンテンツキーを生成する。コンテンツキーはコンテンツ暗号化部１０５に送信される。コンテンツは第１の記憶部３０１からコンテンツ暗号化部１０５に送信され、コンテンツ暗号化部１０５において暗号化される。暗号化されたコンテンツは、サーバ配信処理部１０７を通じて、クライアント端末３５０に配信される。サーバ配信処理部１０７は、前記コンテンツの配信完了を確認すると、課金処理部１０６に通知し、課金処理部１０６が、コンテンツの対価を前記ユーザに対して請求する、課金処理

を行う。

【００２４】クライアント端末３５０では、配信されたコンテンツを、一旦第２記憶部１５４に保存する。この時点でコンテンツはコンテンツキーによって暗号化されている。コンテンツを再生するとき、まずユーザＩＤカード１５５と復号化部１５３とが、お互いの機器が正規のものか否かを確かめるため、相互認証を行う。相互認証によって、正規の機器であることをお互いに確認できた場合のみ、コンテンツキーをユーザＩＤカード１５５から復号化部１５３に送信する。ユーザＩＤカード１５５から復号化部１５３へコンテンツキーを送信する際、例えばＤｉｆｆｉｅ－ＨｅｌｌｍａｎＮの鍵配送を用いてユーザＩＤカード１５５および復号化部１５３との間で第1の共有鍵を作成し、該第1の共有鍵を用いてコンテンツキー自体を暗号化して送信する。その後復号化部１５３において、まず暗号化されたコンテンツキーが、第１の共有鍵を用いて復号され、次にコンテンツ暗号化されたコンテンツが第２の記憶部１５４から復号化部１５３に送信され、復号化部１５３において、コンテンツキーを用いて暗号を復号され、ユーザが利用できるデータに変換される。

【００２５】なお、コンテンツキーには、利用制限情報を付加することもできる。この場合、コンテンツを復号するとき、復号部１５３はコンテンツキーに含まれる利用制限情報を参照し、コンテンツ利用可能の場合のみ復号するとしてもよい。

【００２６】以上のように、本実施の形態１によるコンテンツ配信システムでは、コンテンツはコンテンツＩＤとユーザＩＤとを用いて暗号化され、サーバ３５０からクライアント端末３５０に送信される。ユーザは配信を受ける際、ユーザＩＤカード１５５があればどのクライアント端末でもコンテンツの配信を受けることができ、しかも著作権は保護される。

【００２７】（実施の形態２）図２は本発明におけるコンテンツ配信システムの実施の形態２に係る。図２において４００はコンテンツを配信するサーバであり、該サーバの構成は図１に示すサーバ３００とほぼ同じである。

【００２８】４５０はサーバとネットワーク接続されたクライアント端末である。符号３５１，４５２、および１５４が、クライアント端末４５０の内部機能ブロックを表す。符号３５１は配信されたコンテンツを受信して第２の記憶部１５４に送信し、ユーザＩＤカード１５５からの制御信号をサーバ３００に送信し、サーバ３００からの制御信号を該ユーザＩＤカード１５５に送信するクライアント配信処理部、４５２はユーザＩＤカード１５５と、メモリカード１５６を装着するカードリーダ／ライタ、１５４は配信されたコンテンツを格納する第２の記憶部、１５５はユーザやユーザの使用する機器を識別するユーザ識別情報とコンテンツキーとからなるユーザ情報を格納するユーザＩＤカードである。このユーザＩＤカード１５５は、ユーザが配信を受ける際に必要となる。１５６は配信を受けたコンテンツや、コンテンツの復号に必要となるコンテンツキーを格納できるメモリカードである。１５７は復号再生装置であり、メモリカード１５６を装着することができる。

【００２９】以上のように構成されたコンテンツ配信システムについて、以下、その動作を述べる。いまあるユーザが配信されたコンテンツおよび該コンテンツを復号するためのコンテンツキーをメモリカード１５６にコピーする場面を考える。この場合、第２の記憶部１５４にコンテンツが保存され、ユーザＩＤカード１５５にコンテンツキーがすでに格納されているものとする。また、コンテンツキーには、該コンテンツキー自身のコピー世代情報が付加されているものとする。まず、コンテンツは暗号化された状態でメモリカード１５６にコピーされる。暗号化されたままのコンテンツのメモリカード１５６へのコピーは自由に行ってよい。次にコンテンツキーをメモリカード１５６にコピーする。

【００３０】図５は、コンテンツキーをメモリカード１５６にコピーする処理６００の流れ図を示す。処理６００は処理６０１から６０６で構成される。まず処理６０１において、ユーザＩＤカード１５５とメモリカード１５６の間で、お互いの機器が正規の機器であることを確認する相互認証を行う。前記相互認証に失敗した場合には、メモリカード１５６へのコピーを中止し、処理６００を終了する。前記相互認証に成功すれば、処理６０２において、ユーザＩＤカード１５５とメモリカード１５６でＤｉｆｆｉｅ－ＨｅｌｌｍａｎＮの鍵配送を行い、ユーザＩＤカード１５５とメモリカード１５６との間でコンテンツキーを安全に転送するための第2の共有鍵を作成する。次に処理６０３において、ユーザＩＤカード１５５に格納されているコンテンツキーを参照し、該コンテンツキーのコピー世代がＮ以下であることを確認する。ここで、Ｎは０以上の整数で、それぞれのコンテンツ配信システムにおける最適な値が１つ選ばれる。もし、前記コピー世代値が（Ｎ＋１）以上であった場合には、処理を終了する。前記コピー世代がＮ以下であった場合、次の処理に進む。処理６０４において、コンテンツキーのコピー世代値に１を加える。次に処理６０５においてユーザＩＤカード１５５のコンテンツキーを、処理６０２で作成した前記第2の共有鍵を用いて暗号化する。次に処理６０６において、コンテンツキーをユーザＩＤカード１５５からメモリカード１５６に転送し、メモリカード１５６に格納されていた前記第２の共有鍵を用いて、コンテンツキーを復号する。復号された該コンテンツキーは、ユーザが読み取り不可能な領域に格納される。ユーザが読み取り不可能な領域にコンテンツキーを記録することで、不正コピーを防止する。

【００３１】以上の手続きにより、コンテンツおよびコ

ンテンツキーはメモリカード１５６に記録される。メモリカード１５６を、復号再生端末１５７に装着することで、ユーザＩＤカード１５５がない場合においても、復号再生端末１５７の復号機能により、コンテンツをユーザの利用可能なデータに変換できる。

【００３２】なお、コンテンツキーには、利用制限情報を付加することもできる。この場合、コンテンツを復号するとき、復号再生端末１５７はコンテンツキーに含まれる利用制限情報を参照し、コンテンツ利用可能の場合のみ復号するとしてもよい。

【００３３】以上のように、本実施の形態３によるコンテンツ配信システムは、メモリカード１５６に暗号化されたコンテンツと暗号の解読に必要なコンテンツキーを格納する。コンテンツキーにはコンテンツキー自体のコピー世代情報が付加されており、コンテンツキーのコピー回数を制限する。また、コンテンツキーは、ユーザが読み取り不可能な領域に格納することで、不正にコンテンツキーをコピーすることを防止する。これによりユーザは、メモリカード１５６を復号再生端末１５７に装着することにより、コンテンツをユーザが利用できるデータに復元できる。

【００３４】（実施の形態３）図３は本発明のコンテンツ配信システムにおける実施の形態３に係る。図３において５００はコンテンツを配信するサーバ、３０１はコンテンツとコンテンツ識別情報とを格納する第１記憶部、１０２はコンテンツ識別情報を抽出する抽出部、１０３は各ユーザ毎にユーザＩＤや配信したコンテンツ、およびコンテンツキーなどの情報を保持する情報管理部、１０４はコンテンツの暗号化に用いるコンテンツキーを生成するコンテンツキー生成部、１０５はコンテンツを暗号化するコンテンツ暗号化部、１０６は配信されたコンテンツに相応する対価を配信先のユーザに対し請求し課金処理を行う課金処理部、１０７は暗号化部の出力を、ネットワークを通じてクライアント端末５５０に配信し、またクライアント端末からの送信情報をコンテンツキー生成部と課金処理部１０６に出力するサーバ配信処理部である。

【００３５】符号５５１，１５２，１５３および１５４が、クライアント端末５５０の内部機能ブロックを表す。５５１は配信されたコンテンツを受信して第２の記憶部に送信し、ユーザＩＤカード１５５からの制御信号をサーバ５００側に送信し、サーバ５００側からの制御信号をユーザＩＤカード１５５に送信するクライアント配信処理部、１５２はユーザＩＤカード１５５と、メモリカード１５６を装着するカードリーダ／ライタ、１５３は配信されたコンテンツの暗号を復号する復号化部、１５４は配信されたコンテンツを格納する第２記憶部、１５５はユーザやユーザの使用する機器を識別するユーザ識別情報とコンテンツキーとからなるユーザ情報を格納するユーザＩＤカード１５５である。ユーザＩＤカード１５５は、ユーザが配信を受ける際に必要となる。１５６は配信を受けたコンテンツや、コンテンツの復号に必要となるコンテンツキーを格納できるメモリカードである。１５７は復号再生装置であり、メモリカード１５６を装着することができる。

【００３６】図８は、情報管理部１０３で管理されるユーザ情報データベースの一例である。情報管理部１０３は実施の形態１と同じように、配信サービスを提供しているユーザ毎に、ユーザＩＤと、コンテンツＩＤ、最新配信日時、著作権期限、コンテンツ使用期限、価格、配信回数、コンテンツキー情報などを管理する。

【００３７】以上のように構成されたコンテンツ配信システムについて、以下、その動作を述べる。実際に配信を行う場面については実施の形態１とほぼ同じである。サーバ５００では、全ユーザの配信コンテンツ履歴情報などのユーザ情報を図８に示すようにデータベース管理している。サーバ５００は、ユーザがすでに配信を受けたコンテンツを再配信することができるようにする。ここで、第２の記憶部１５４などに保存されている暗号化コンテンツだけが壊れている場合には、前回の配信に用いたコンテンツキーをもう一度使用してコンテンツ暗号化してもよい。しかしながら、コンテンツキーが壊れている場合には、同じコンテンツキーで暗号化を行ってもユーザは復号できないため、消失したものとは異なる、第２のコンテンツキーをユーザＩＤカード１５５とコンテンツキー生成部１０４との間で作成する。その後、コンテンツを第２のコンテンツキーで暗号化し、ユーザに配信する。コンテンツキーの作成履歴を情報管理部１０３で管理しておくことで、ユーザが配信を受けたコンテンツに対するコンテンツキー作成回数を制限し、不正コピーを防止する。

【００３８】図６の処理７００は、ユーザ側で、例えばハードウェア故障によってコンテンツが消失してしまった場合に、再配信を行う場合の処理の流れを表す。処理７００は処理７０１から処理７０８で構成される。まず、ユーザがサーバ５００にアクセスする。次に処理７０１において、コンテンツキー生成部１０４とユーザＩＤカード１５５との間でお互いが正規の機器同士であることを確認する相互認証を行う。認証に失敗した場合、処理７００は終了する。認証に成功すれば、次にユーザは処理７０２に示す通報を行う。ここでユーザはカードを破損したことを伝え、現在消失してしまったあるコンテンツを再配信したいとサーバ５００に知らせる。処理７０３において図８に示すユーザ情報データベースの中の、配信曲履歴情報を参照する。処理７０４において、ユーザが配信を要求しているコンテンツに対するこれまでの配信回数を確認し、これまでの配信回数がＭ回以下であれば配信要求を許可し、（Ｍ＋１）回以上であれば配信要求を棄却し、処理７００は終了する。ここでＭは１以上の整数とし、それぞれのコンテンツ配信システム

に最適となる値が１つ選ばれる。次に、処理７０５において、コンテンツキー生成部１０４とユーザＩＤカード１５５との間で、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎの鍵配送により第２のコンテンツキーを配布する。処理７０６では、第２のコンテンツキーを用いてコンテンツを暗号化し、次の処理に進む。処理７０７において、暗号化されたコンテンツを再配信し、処理７０８において、ユーザの配信コンテンツ履歴情報の、コンテンツの配信回数に１を加える。

【００３９】以上のように、本実施の形態３によるコンテンツ配信システムは、サーバはユーザや該ユーザに配信した情報を管理する。ユーザに配信したコンテンツが、ハードウェア故障などの原因によって消失してしまった場合、サーバはユーザの情報を管理しているので、該ユーザが配信を受けた曲を再配信することを可能とする。

【００４０】（実施の形態４）図４は、本発明におけるコンテンツ配信システムの実施の形態４に係る。図４において１００はコンテンツを配信するサーバであり、符号１０１，１０２，１０３，１０４，１０５，１０６および１０７がサーバ１００の内部機能ブロックを表す。１０１はコンテンツとコンテンツ識別情報（以下、コンテンツＩＤ）とを格納する第１の記憶部、１０２はユーザの配信要求にしたがって、ユーザ所望のコンテンツに対するコンテンツＩＤと、コンテンツの著作権期限や対価などを表すコンテンツ属性情報とを抽出する抽出部、１０３は各ユーザ毎に、ユーザの識別情報（以下、ユーザＩＤ）と、配信したコンテンツと、該コンテンツのコンテンツキーなどの情報とを保持する情報管理部、１０４はコンテンツの暗号化に用いるコンテンツキーを生成するコンテンツキー生成部、１０５はコンテンツを暗号化するコンテンツ暗号化部、１０６は配信されたコンテンツに相応する対価を配信先のユーザに対し請求処理を行う、課金処理部、１０７はサーバにおける配信処理を行う配信処理部である。

【００４１】符号１５０はサーバとネットワーク接続されたクライアント端末である。符号１５１、１５２、１５３、１５４が、リモート端末１５０の内部機能ブロックを表す。１５１はクライアント端末側の配信処理を行うクライアント配信処理部、１５２はクライアント端末にユーザＩＤカードやメモリカード１５６を装着するカードリーダ／ライタ、１５３は暗号化されたコンテンツを復号する復号化部、１５４は暗号化されたコンテンツを格納する第２の記憶部、１５５はユーザが配信を受ける際に必要となるユーザＩＤカード、１５６はメモリカード、１５７は復号再生装置であり、メモリカード１５６を装着することができる。

【００４２】図８は、情報管理部１０３で管理されるユーザ情報データベースの一例である。情報管理部１０３は、配信サービスを提供しているユーザ毎に、ユーザＩＤと、コンテンツＩＤ、最新配信日時、著作権期限、コンテンツ使用期限、価格、配信回数、コンテンツキー情報などを管理する。以上のように構成されたコンテンツ配信システムについて、以下その動作を述べる。

【００４３】図７は、コンテンツの著作権が切れた場合の処理８００の流れを表す。処理８００は、処理８０１から８０７で構成される。まず処理８０１において、著作権の情報は情報管理部１０３に送信され、情報管理部１０３において、ユーザ情報データベースに反映される。次に処理８０２において、配信されたコンテンツの管理方法が自動であるか、ユーザの指示を待つかを判断する。管理方法が自動（Ｙｅｓ）であった場合処理８０４に移る。管理方法が自動でなかった（Ｎｏ）場合、処理８０３においてコンテンツの属性情報が変化してから初めて、ユーザがサーバ１００にアクセスしたことをサーバ１００が認識した後に、処理８０４に移る。処理８０４において、ユーザに、コンテンツの著作権期限が切れたことを伝える。ユーザは処理８０５において、暗号化解除をするかしないかをサーバ１００に伝える。暗号解除の必要がない（Ｎｏ）場合には処理を終了する。

【００４４】ユーザが暗号化解除を要求した（Ｙｅｓ）場合には処理８０６に移る。処理８０６において、サーバ１００は情報管理部１０３に格納してあって、前記コンテンツのコンテンツキーをユーザに送信する。このとき、配信を受けたコンテンツキーは、ユーザが自由に扱うことができるように、暗号化をせずに送信する。ユーザは、そのコンテンツキーを用いてコンテンツを自由に復号できる。これにより、著作権が切れた場合、ユーザは、コンテンツの暗号を復号し、ユーザが利用できるデータに変換した上で、自由にコピーすることが可能となる。なお、本実施の形態で示した著作権切れの場合でも、対価は支払わなければならないとき、処理８００を実行しないようにしてもよい。この場合、対価が０円となったとき、処理８００を実行できるとする。

【００４５】実施の形態４によるコンテンツ配信システムは、サーバがユーザに配信したコンテンツの対価や著作権などの属性情報を管理する。ユーザに配信したコンテンツの著作権が切れた場合、サーバはユーザに通知し、コンテンツキーを送信する。コンテンツキーを用いれば、ユーザは、コンテンツの暗号化解除が可能となる。これらのことから、サーバは、ユーザに配信したコンテンツの利用制限解除をメンテナンスできる。

【００４６】

【発明の効果】以上説明したところから明らかなように、本発明は、ユーザが配信を希望するコンテンツは、ユーザＩＤと、コンテンツＩＤとを用いて暗号化される。ユーザは、ユーザＩＤカード１５５があれば、いかなるクライアント端末でもコンテンツ配信を受けることができ、著作権も保護される。

【００４７】また、本発明は、ユーザ情報をサーバで管

理することにより、ユーザが何らかの形でコンテンツを消失してしまった場合には、サーバは、回数を限定してコンテンツの再配信することができる。

【００４８】また、本発明は、ユーザが配信を受けたコンテンツの著作権が切れた場合、サーバはユーザに該コンテンツの著作権が切れたことを告知し、必要に応じてコンテンツキーをユーザに配布することで、ユーザは暗号化されたコンテンツを復号し、自由に取り扱うことができるようになる。これらにより、配信を受けるユーザの利便性が向上したコンテンツ配信システムを提供することが奏される。

【図面の簡単な説明】

【図１】本発明の実施の形態１に係るコンテンツ配信システムの機能ブロック図

【図２】本発明の実施の形態２に係るコンテンツ配信システムの機能ブロック図

【図３】本発明の実施の形態３に係るコンテンツ配信システムの機能ブロック図

【図４】本発明の実施の形態４に係るコンテンツ配信システムの機能ブロック図

【図５】本発明のコンテンツ配信システムにおけるメモリカードにコンテンツキーを複写する場合の説明に用いるフローチャート

【図６】本発明のコンテンツ配信システムにおける、カード破損による再配信を説明するフローチャート

【図７】本発明のコンテンツ配信システムにおける、著作権期限切れの場合の説明に用いるフローチャート

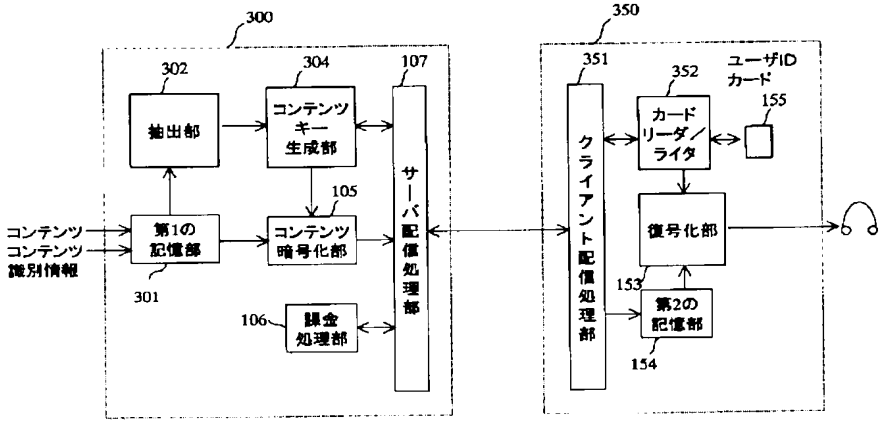
【図８】本発明のコンテンツ配信システムにおける、ユーザ情報管理データベースの一例の表を示す図

【図９】従来のコンテンツ配信システムの一例を説明する機能ブロック図

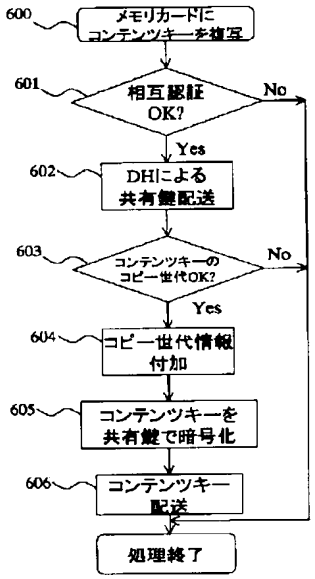
【符号の説明】

１０，１００，３００，４００，５００　サーバ
１１　コンテンツ蓄積部
１４　機器キーデータベース
１５　機器暗号化部
１６　課金マネージャ
１７，２１　通信マネージャ
２０，１５０，３５０，４５０，５５０　クライアント端末
２３　リモート処理マネージャ
２４　データ蓄積部
２５　ＩＣカード
１０１，３０１　第１の記憶部
１０２，３０２　抽出部
１０３　情報管理部
１０４，１２，３０４　コンテンツキー生成部
１０５，１３　コンテンツ暗号化部
１０６　課金処理部
１０７　サーバ配信処理部
１５１，３５１，５５１　クライアント配信処理部
２２，１５２，３５２，４５２　カードリーダ／ライタ
１５３　復号化部
１５４　第2の記憶部
１５５　ユーザＩＤカード
１５６　メモリカード
１５７　復号再生端末

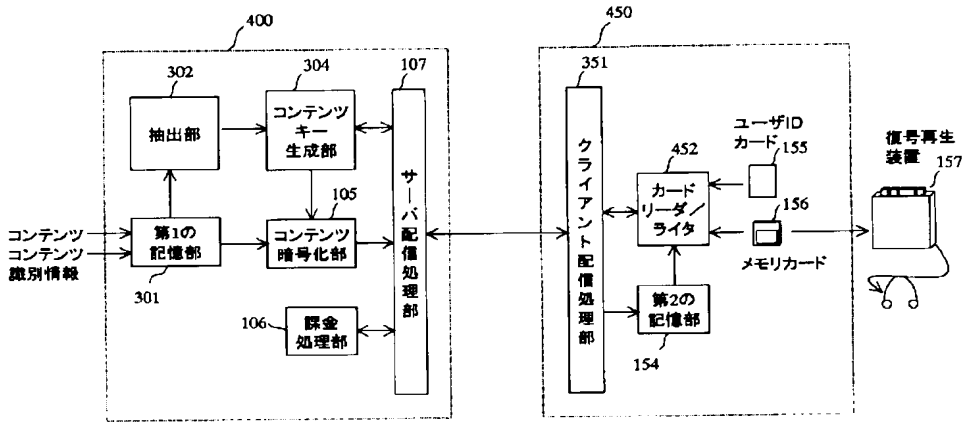
【図１】



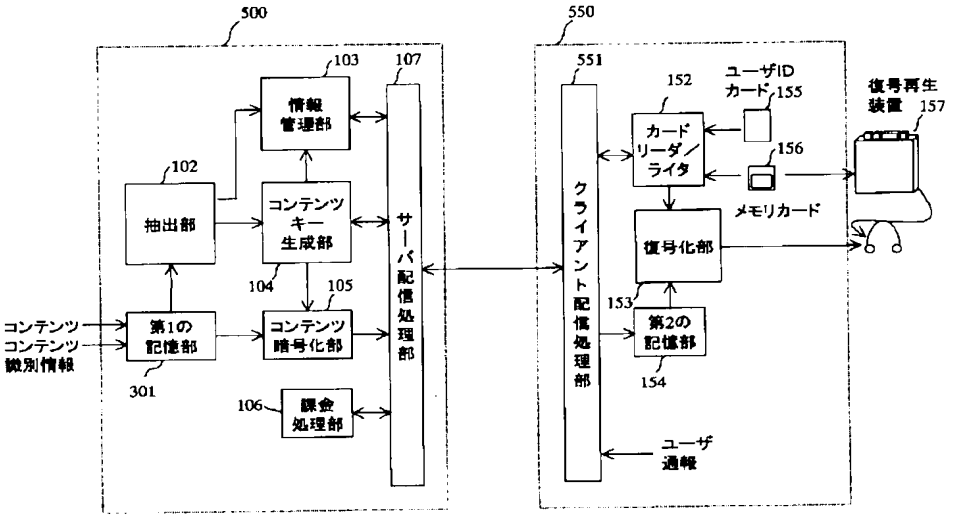
【図５】



【図２】



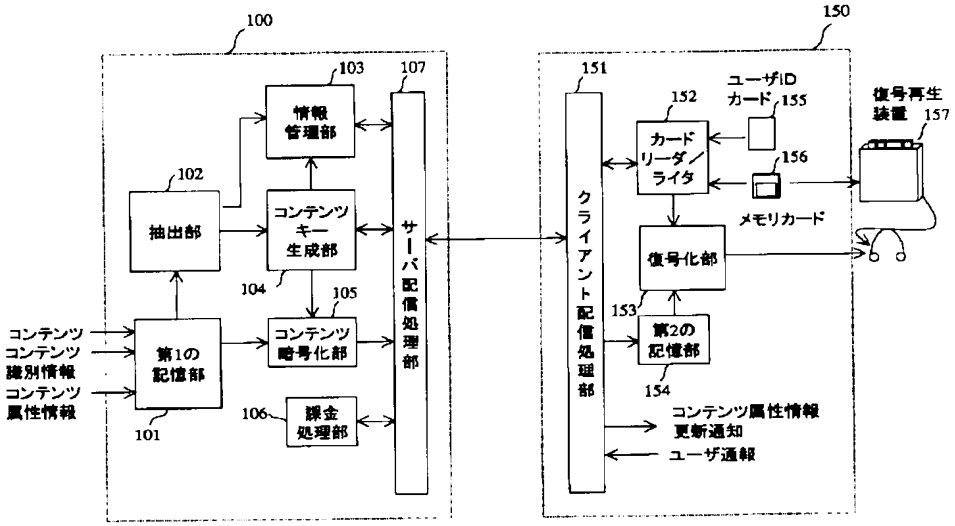
【図３】



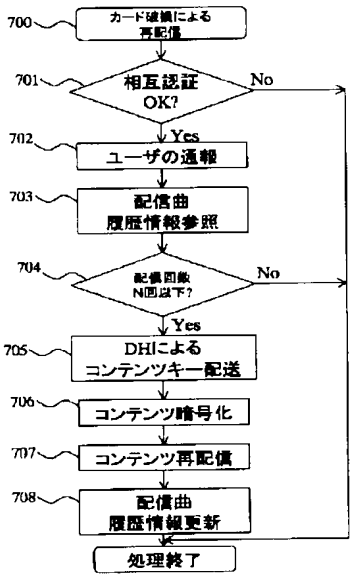
【図８】

ユーザ毎	ユーザID	配信コンテンツ識別情報(ID)	最新配信日時	著作権期限	コンテンツ使用期限	価格	配信回数	コンテンツキー
ユーザA	23498675	YS-GU34-a	1998.12.30 17:00	2049.11.30	なし	700円	1回目	Key A (非公開)
		TM-GQ40-a	2000.01.02 13:30	期限切れ	なし	1500円	1回目	Key B (非公開)
		YS-GU34-a	2000.01.05 14:00	2049.11.30	なし	700円	2回目	Key C (非公開)
ユーザB	52382975	TS-TW90-a	2000.01.15 03:00	2048.01.31	2000.12.31	3000円	3回目	Key D (非公開)
ユーザC	835245893							
		HW-IP58-a	2000.02.01 14:30	1971.09.30 (期限切れ)	なし	0円	1回目	Key E (公開)
ユーザD	9201135	HW-IP58-a	2000.02.01 14:30	1971.09.30 (期限切れ)	なし	0円	1回目	Key E (公開)
...	...	...	...	...		...	...	...

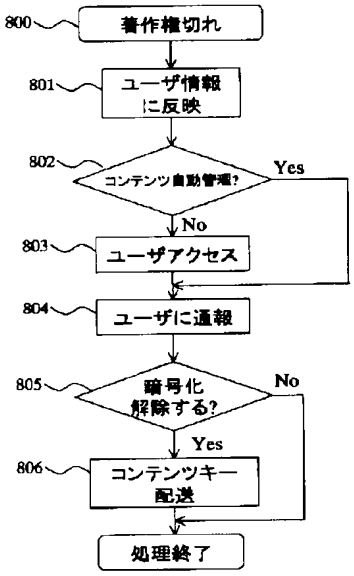
【図４】


100
150
103
107
151
ユーザID
カード
155
152
復号再生
装置
157
情報
管理部
カード
リーダ／
ライタ
156
102
抽出部
コンテンツ
キー
生成部
サーバ配信処理部
クライアント配信処理部
メモリカード
復号化部
104
105
153
コンテンツ
コンテンツ
識別情報
コンテンツ
属性情報
第1の
記憶部
コンテンツ
暗号化部
第2の
記憶部
154
106
課金
処理部
101
コンテンツ属性情報
更新通知
ユーザ通報

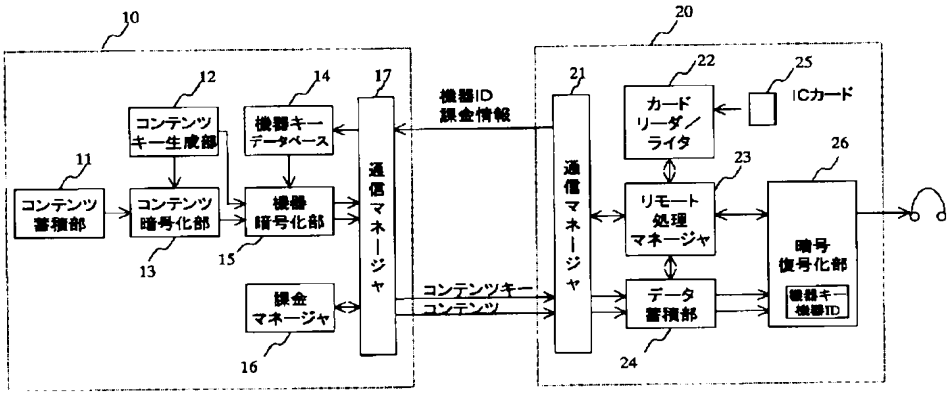
【図６】


700
カード破損による
再配信
701
相互認証
OK?
No
Yes
702
ユーザの通報
703
配信曲
履歴情報参照
704
配信回数
N回以下?
No
Yes
705
DHによる
コンテンツキー配送
706
コンテンツ暗号化
707
コンテンツ再配信
708
配信曲
履歴情報更新
処理終了

【図７】


800
著作権切れ
801
ユーザ情報
に反映
802
コンテンツ自動管理?
Yes
No
803
ユーザアクセス
804
ユーザに通報
805
暗号化
解除する?
No
Yes
806
コンテンツキー
配送
処理終了

【図９】



フロントページの続き

(51) Int. Cl.[7]		識別記号
Ｇ１０Ｋ	15/02	
Ｈ０４Ｌ	9/10	
	9/32	
Ｈ０４Ｎ	7/16	
	7/173	６４０

Ｆ Ｉ		ﾃｰﾏｺｰﾄﾞ（参考）
Ｇ１０Ｋ	15/02	
Ｈ０４Ｎ	7/16	Ｃ
	7/173	６４０Ａ
Ｈ０４Ｌ	9/00	６２１Ａ
		６７３Ａ
		６７３Ｅ

Ｆターム（参考） 5B085 AC04 AE02 AE12 AE29
5C064 BA07 BB01 BC01 BC06 BC17
BC18 BC22 BC25 BC27 BD02
BD09 CC01
5J104 AA12 EA04 EA18 EA25 EA28
EA33 KA01 NA02 NA03 NA35
NA36 NA38 PA11